IN THE CLAIMS:

1. (currently amended) A computer network comprising:

a server system;

a client system~~, the server system and the client system executing processes to provide security mechanisms for securing traffic communication between the two systems, the processes including key exchange processes executed when the client system is in an operational state~~;

logic for detecting whether the client system is in an operational state;

logic for executing a first key exchange process between the server system and the client system to produce results;

a storage device at the client system for storing the results of the first key exchange process[[es]];

logic for inhibiting the stored results of the first key exchange process from being updated until a successful execution of ~~another~~ a second ~~set of~~ key exchange process[[es]] between the server system and the client system;

logic for updating the stored results of the first key exchange process if the execution of the ~~other~~ second ~~set of~~ key exchange process[[es]] is successful; and

logic ~~for updating the stored results of the key exchange if the execution of the other set of key exchange processes is successful; and logic for using results stored in the memory~~ to secure ~~the~~ traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational.

2. (currently amended) The computer network of claim 1, wherein the logic for inhibiting the stored results of the first key exchange process from being updated is embodied in the client system.

3. (currently amended) The computer network of claim 1, wherein the logic for inhibiting the stored results of the first key exchange process from being updated is embodied in the server system.

Claims 4 - 5 (cancelled).

6. (currently amended) The computer network of claim 1, further ~~comprising~~ including logic for allowing the traffic communication between the server system and the client system to be sent without security.

7. (original) The computer network of claim 1, wherein the client system is a network device.

8. (original) The computer network of claim 1, wherein the storage device is at least one of an Ethernet device, a coprocessor connected to an Ethernet device, and non-volatile storage that is part of an Ethernet device.

9. (currently amended) The computer network of claim 1, wherein the logic for inhibiting the stored results of the first key exchange process from being updated includes:

logic for sending a signal acknowledging the successful execution of another set of key exchange processes; and

logic for sending a signal confirming receipt of the acknowledgement signal.

10. (currently amended) The computer network of claim 1, wherein the server system contains a storage device for storing the results of the first key exchange

processes and the second key exchange process.

11. (currently amended) The computer network of claim 1, further comprising logic for switching the server system to a second server system in the computer network if the server system becomes non-operational, [[the]] security mechanisms securing traffic communication between the second server system and the client system.

Claims 12 - 19 (cancelled).

20. (currently amended) A method of providing security mechanisms for securing traffic communication between a server system and a client system, the method comprising:

detecting whether the client system is in an operational state;

executing first key exchange processes between the server system and the client system when if the client system enters is in the operational state;

storing the results of the first key exchange processes into the client system;

inhibiting the stored results from being updated until a successful execution of a second set of key exchange processes between the server system and the client system;

updating the stored results with the results obtained from the second set of key exchange processes if the execution of the second set of key exchange processes is successful; and

using either the stored results or the updated results of the first key exchange processes to secure the traffic communication depending on whether if the second set of key exchange processes is are not successful if because the client system becomes

non-operational.

Claims 21 and 22 (cancelled).

23. (currently amended) The method of claim 20, further ~~comprising the step of~~ including allowing the traffic communication between the server system and the client system to be sent without security.

24. (currently amended) The method of claim 20, wherein the results of the first key exchange processes and the second key exchange processes are stored into at least one of a network device, a coprocessor connected to a network device, and non-volatile storage that is part of a network device.

25. (currently amended) The method of claim 20, wherein ~~the step of~~ inhibiting the stored results of the first key exchange processes from being updated includes:

sending a signal acknowledging the successful execution of the second ~~set of~~ key exchange processes; and

sending a signal confirming receipt of the acknowledgement signal.

26. (currently amended) The method of claim 20, further ~~comprising the step of~~ including storing the results of the first key exchange processes and the second key exchange processes into the server system.

27. (currently amended) The method of claim 20, further ~~comprising the step of~~ including switching the server system to a second server system in the computer network if the server system becomes non-operational, the security mechanisms securing traffic communication between the second server system and the client system.

28. (new) The method of claim 20, wherein using the stored results to secure

the traffic communication further includes transmitting management Internet Protocol-based packets from the server system to the client system, if the client system is determined to be non-operational, to perform diagnostic operations on the client system.

29. (new) The method of claim 28, wherein the transmission of management IP-based protocol packets causes the client system to re-boot.

30. (new) The method of claim 29, wherein the management IP-based protocol packets are remote management and control protocol (RCMP) packets.

31. (new) The network system of claim 1, further including a plurality of client systems coupled to the server system, each of the plurality of client systems including a security parameter, wherein the server system includes a non-volatile storage for storing the security parameter for each of the plurality of client systems.

32. (new) A client system, comprising:

logic for executing a first key exchange process between a server and the client system to product results;

a storage device to store the results of the first key exchange process;

logic for inhibiting the stored results of the first key exchange process from being updated until a second key exchange process is successful;

logic for updating the stored results of the first key exchange process if execution of second key exchange process is successful; and

logic to secure the traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-

operational.

33. (new) The client system of claim 32, further including logic for allowing the traffic communication between the server system and the client system to be sent without security.

34. (new) The client system of claim 32, wherein the logic for inhibiting the stored results of the first key exchange process from being updated includes logic for sending a signal acknowledging the successful execution of another set of key exchange processes; and

logic for sending a signal confirming receipt of the acknowledgement signal.

35. (new) The client system of claim 32, wherein the client system is a network device.

36. (new) The client system of claim 32, wherein the storage device is at least one of an Ethernet device, a coprocessor connected to the Ethernet device, and a non-volatile storage that is part of the Ethernet device.

37. (new) The client system of claim 32, wherein the securing of the communication traffic further includes logic for receiving management Internet Protocol-based packets from the server system if the client system is determined to be non-operational to perform diagnostic operations on the client system.

38. (new) A computer readable medium, the computer readable medium including computer readable instructions encoded thereon, which when executed cause a client system to:

execute a first key exchange process between a server system and the client system if the client system is in an operational state;

store results of the first key exchange process in the client system;

inhibit the stored results from being updated until a successful execution of a second key exchange process between the server system and the client system; and

use the stored results of the first key exchange process to secure the traffic communication if the second key exchange process is not successful because the client system is non-operational.

39. (new) The computer readable medium of claim 38, further including computer readable instructions encoded thereon, which when executed cause the client system to allow the traffic communication between the server system and the client system to be sent without security.

40. (new) The computer readable medium of claim 38, wherein the instructions to inhibit the stored results of the first key exchange process from being updated include sending a signal acknowledging the successful execution of the second key exchange process; and

sending a signal confirming receipt of the acknowledgment signal.

41. (new) The computer readable medium of claim 38, further including computer readable instructions encoded thereon, which when executed cause the client system to switch the server system to a second server system in the computer network if the server system becomes non-operational, where the second server system includes security mechanisms for securing traffic communication between the second server system and the client system.